Reference 2

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－340255

(43)公開日　平成10年(1998)12月22日

(51)Int.Cl.[6]	識別記号	FI	
G06F 15/00	330	G06F 15/00	330E
G09C 1/00	640	G09C 1/00	640E
H04L 9/32		H04L 9/00	675A
			675B

審査請求　有　請求項の数4　OL　（全７頁）

(21)出願番号　特願平9－151761

(22)出願日　平成９年(1997)６月10日

(71)出願人　000164449
九州日本電気ソフトウェア株式会社
福岡市早良区百道浜２丁目４－１　NEC九州システムセンター

(72)発明者　後藤　正人
福岡県福岡市早良区百道浜２－４－１　九州日本電気ソフトウェア株式会社内

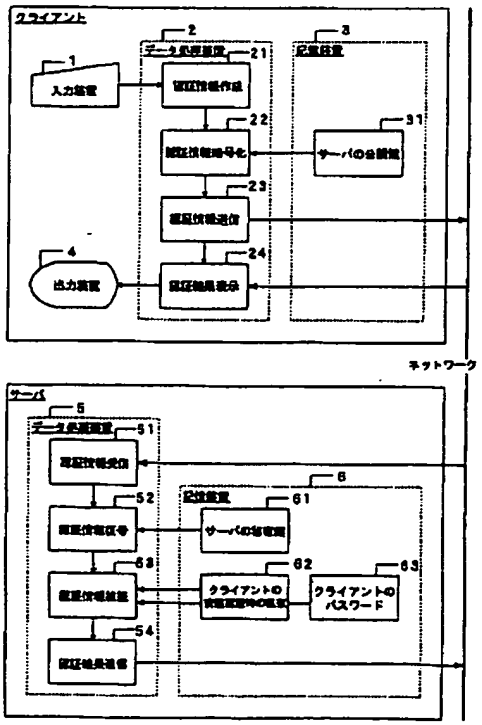
(74)代理人　弁理士　岩佐　義幸

(54)【発明の名称】　ネットワーク利用者認証方式

(57)【要約】

【課題】　ネットワーク利用者認証システムにおける第三者によるクライアントなりすましを防止する。

【解決手段】　クライアントの入力装置１から与えられた利用者識別子、パスワード、有効時間から、認証情報作成２１が認証情報有効期限と乱数を作成して、認証情報を作成する。認証情報暗号化２２が認証情報をサーバの公開鍵で暗号化し、認証情報送信２３が暗号化された認証情報をサーバへ送信する。サーバの認証情報受信５１が暗号化された認証情報を受信し、認証情報復号５２が暗号化された認証情報をサーバの秘密鍵で復号する。認証情報検証５３が認証情報の認証情報有効期限が期限切れでないこと、認証情報の乱数が前回認証時と同じでないことを検証した後、パスワードを検証する。認証結果送信５４が認証結果をクライアントに送信し、認証結果表示２４が認証結果を出力装置に表示する。



1

【特許請求の範囲】
【請求項１】ネットワーク上のサーバがクライアントを認証するネットワーク利用者認証方式において、
クライアントが、認証情報に認証情報有効期限と乱数を追加する認証情報作成手段を備え、
サーバが、認証情報の認証情報有効期限と乱数を検証する認証情報検証手段を備えることを特徴とするネットワーク利用者認証方式。
【請求項２】ネットワーク上のサーバがクライアントを認証するネットワーク利用者認証システムにおいて、
クライアントは、
キーボード等の入力装置と、
サーバの公開鍵をあらかじめ記憶している記憶装置と、
ディスプレイ装置等の出力装置と、
前記入力装置から与えられた利用者識別子、パスワード、有効時間を基にして認証情報を作成し、作成した認証情報を前記サーバの公開鍵で暗号化し、暗号化された認証情報をサーバへ送信し、サーバから受信した認証結果を前記出力装置に表示するデータ処理装置と、を備え、
サーバは、
サーバの秘密鍵と、クライアントの前回認証時の乱数と、クライアントのパスワードをあらかじめ記憶している記憶装置と、
クライアントから暗号化された認証情報を受信し、暗号化された認証情報を前記サーバの秘密鍵で復号し、認証情報の認証情報有効期限が期限切れでないことと、認証情報の乱数が前記前回認証時の乱数と同じでないことと、前記パスワードを検証し、認証結果をクライアントに通知するデータ処理装置と、を備えることを特徴とするネットワーク利用者認証方式。
【請求項３】クライアントがサーバに送信する認証情報に認証情報有効期限と乱数付加し、サーバがクライアントから受信した認証情報の認証情報有効期限と乱数を検証することを特徴とするネットワーク利用者認証方法。
【請求項４】クライアントの入力された利用者識別子、パスワード、有効時間から、認証情報有効期限と乱数を作成して、認証情報を作成し、
作成された認証情報をサーバの公開鍵で暗号化し、
暗号化された認証情報をサーバへ送信し、
暗号化された認証情報をサーバにて受信し、
暗号化された認証情報をサーバの秘密鍵で復号し、
認証情報の認証情報有効期限が期限切れでないこと、認証情報の乱数が前回認証時と同じでないことを検証した後、パスワードを検証し、
認証結果をクライアントに送信し、
認証結果をクライアントの出力装置に表示することを特徴とするネットワーク利用者認証方法。
【発明の詳細な説明】
【０００１】

2

【発明の属する技術分野】本発明は、ネットワーク利用者認証方法に関し、特にクライアントがサーバに送信する一方向の認証情報のみでサーバがクライアントを認証する機能を有するネットワーク認証方法に関する。
【０００２】
【従来の技術】従来、この種のネットワーク利用者認証方法は、ネットワーク上のサーバがクライアントを認証するために用いられている。従来のネットワーク利用者認証方法の一例が、特開平０７－３２５７８５号公報に記載されている。この公報に記載されたネットワーク利用者認証方法は、認証情報として利用者識別子とパスワードをクライアントからサーバに送信し、サーバは該当する認証情報が存在することを確認して利用者認証を行うシステムにおいて、ネットワーク上の認証情報を保護するために、クライアントは、認証情報をサーバの公開鍵方式の公開鍵で暗号化してサーバへ送信し、サーバは、自分の秘密鍵でそれを復号して認証情報を取り出す。また、クライアントがサーバへ認証情報を送信する前に、サーバがクライアントに乱数をクライアントへ送信し、クライアントが認証情報に乱数を含めてサーバの公開鍵で暗号化してサーバへ送信し、サーバは復号した乱数が先に送信した乱数と同じであることを確認する。
【０００３】
【発明が解決しようとする課題】従来の技術において、サーバの公開鍵で暗号化された認証情報を第三者が取得した場合、その者が認証情報の内容を知ることは不可能であるが、クライアントになりすましてその認証情報をサーバへ送信して認証を得ることは可能である。それは、認証情報の内容が毎回同じであるためである。
【０００４】このような問題点を解決するために、あらかじめサーバからクライアントへ乱数を送信し、クライアントが認証情報にその乱数を含めてサーバに送信する方法では、サーバとクライアント間で二方向の通信が必要となる。それは、認証情報の一意性を実現する情報をクライアントがサーバから得ているためである。
【０００５】本発明の目的は、クライアントからサーバへ送信する認証情報の再利用が不可能となるネットワーク利用者認証方法を提供することにある。
【０００６】また本発明の他の目的は、クライアントからサーバへ送信する認証情報が一方向のみでセキュリティを確保できるネットワーク利用者認証方法を提供することにある。
【０００７】
【課題を解決するための手段】本発明のネットワーク利用者認証方式は、クライアントからサーバへ送信する認証情報に認証情報有効期限と乱数を追加し、サーバがそれを検証する。より具体的には、ネットワーク上のサーバがクライアントを認証するネットワーク利用者認証方式において、クライアントは、キーボード等の入力装置と、サーバの公開鍵をあらかじめ記憶している記憶装置

と、ディスプレイ装置等の出力装置と、前記入力装置から与えられた利用者識別子、パスワード、有効時間を基にして認証情報を作成し、作成した認証情報を前記サーバの公開鍵で暗号化し、暗号化された認証情報をサーバへ送信し、サーバから受信した認証結果を前記出力装置に表示するデータ処理装置と、を備え、サーバは、サーバの秘密鍵と、クライアントの前回認証時の乱数と、クライアントのパスワードをあらかじめ記憶している記憶装置と、クライアントから暗号化された認証情報を受信し、暗号化された認証情報を前記サーバの秘密鍵で復号し、認証情報の認証情報有効期限が期限切れでないことと、認証情報の乱数が前記前回認証時の乱数と同じでないことと、前記パスワードを検証し、認証結果をクライアントに通知するデータ処理装置と、を備えることを特徴とする。

【０００８】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【０００９】図１は、本発明のネットワーク利用者認証方式の実施の形態を示すブロック図である。図１に示すネットワーク利用者認証方式は、クライアントのキーボード等の入力装置１と、プログラム制御により動作するデータ処理装置２と、情報を記憶する記憶装置３と、ディスプレイ装置等の出力装置４と、サーバのプログラム制御により動作するデータ処理装置５と、情報を記憶する記憶装置６とを備えている。

【００１０】記憶装置３は、サーバの公開鍵３１をあらかじめ記憶している。記憶装置６は、サーバの秘密鍵６１と、クライアントの前回認証時の乱数６２と、クライアントのパスワード６３をあらかじめ記憶している。

【００１１】データ処理装置２は、認証情報作成２１と、認証情報暗号化２２と、認証情報送信２３と、認証結果表示２４とを備えている。認証情報作成２１は、入力装置１から与えられた利用者識別子、パスワード、有効時間を基にして認証情報を作成する。認証情報暗号化２２は、認証情報をサーバの公開鍵で暗号化する。認証情報送信２３は、暗号化された認証情報をサーバへ送信する。認証結果表示２４は、サーバからの認証結果を受信し、それを出力装置４に表示する。

【００１２】データ処理装置５は、認証情報受信５１と、認証情報復号５２と、認証情報検証５３と、認証結果送信５４とを備えている。認証情報受信５１は、クライアントから暗号化された認証情報を受信する。認証情報復号５２は、暗号化された認証情報をサーバの秘密鍵で復号する。認証情報検証５３は、認証情報の有効期限と、乱数の再現性と、パスワードとを検証する。認証結果送信５４は、認証結果をクライアントに通知する。

【００１３】本発明の実施の形態の特徴は、クライアントからサーバへの一方向の通信で、サーバがクライアントを認証することにある。クライアントの認証情報作成２１が、認証情報として、認証情報の有効期限と、乱数とを作成し、サーバの認証情報検証５３が、クライアントの認証条件として、現時刻が認証情報の有効期限を過ぎていないこと、乱数が前回と同じでないことを検証する。

【００１４】次に、図１および図２を参照して、本発明の実施の形態の動作について説明する。図２は、本発明の実施の形態の動作を説明するフローチャートである。入力装置１から与えられた利用者識別子、パスワード、有効時間は、認証情報作成２１に供給される。認証情報作成２１は、現時刻に有効時間を加算して認証情報有効期限を作成し、乱数を生成する（ステップＡ１，Ａ２）。認証情報暗号化２２は、セッション鍵（共通鍵方式の暗号鍵）となる乱数を生成し、認証情報（利用者識別子、パスワード、認証情報有効期限、乱数）を暗号化し、サーバの公開鍵３１を用いてセッション鍵を暗号化する（ステップＡ３，Ａ４，Ａ５）。認証情報送信２３は、暗号化された認証情報と暗号化されたセッション鍵をサーバへ送信する（ステップＡ６）。

【００１５】認証情報受信５１は、クライアントの暗号化された認証情報と暗号化されたセッション鍵を受信する（ステップＢ１）。認証情報復号５２は、暗号化されたセッション鍵をサーバの秘密鍵６１を用いて復号し、暗号化された認証情報をセッション鍵を用いて復号する（ステップＢ２，Ｂ３）。認証情報検証５３は、現時刻が認証情報有効期限を過ぎていないこと、クライアントの前回認証時の乱数６２を用いて認証情報の乱数が前回と異なること、クライアントのパスワード６３を用いて認証情報のパスワードが正しいことを検証する（ステップＢ４，Ｂ５，Ｂ６）。

【００１６】認証結果送信５３は、認証完了あるいは認証失敗をクライアントへ送信する（ステップＢ７，Ｂ８）。認証結果表示２４は、出力装置４にサーバから受信した認証結果を表示する（ステップＡ７）。

【００１７】次に、本発明の実施例について詳細に説明する。図３は、本発明の一実施例を示すブロック図である。図３を参照すると、入力装置１より有効時間が認証情報作成２１に供給された場合、認証情報作成２１は、認証情報として、現時刻に有効時間を加算して、認証情報有効期限を作成し、乱数を生成する。認証情報検証５３は、現時刻を取得し、認証情報有効期限を過ぎてないことと、認証情報の乱数がクライアントの前回認証時の乱数６２と異なることを検証する。

【００１８】たとえば入力装置１より有効時間として１０分が認証情報作成２１に供給された場合、認証情報作成２１は、認証情報として、現時刻（１９９７年３月２５日１１時２０分）に１０分を加算して、認証情報有効期限（１９９７年３月２５日１１時３０分）を作成し、乱数（６５４３２１０９８７６５４３２１）を生成する。認証情報検証５３は、現時刻（１９９７年３月２５

日１１時２５分）を取得し、認証情報有効期限を過ぎてないことと、認証情報の乱数（６５４３２１０９８７６５４３２１）がクライアントの前回認証時の乱数６２（１２３４５６７８９０１２３４５６）と異なることを検証する。

【００１９】本実施の形態は、クライアントがサーバへ送信する認証情報に有効期限と乱数を付加することで、認証情報の一意性が向上する。たとえば、第三者がネットワーク上でこの認証情報を取得し、クライアントになりすまして、認証情報をサーバへ送信しても、認証情報の有効期限が切れていたり、すでに同じ乱数で認証済みとなっている可能性が高い。また、認証情報の一意性を高めるために、あらかじめサーバからクライアントに乱数を送信しておき、クライアントが認証情報としてそれをサーバに送信する二方向のネットワーク認証方法があるが、本実施の形態は、同レベルの認証が一方向で実現でき、効率的である。

【００２０】

【発明の効果】以上説明したように本発明は、クライアントが認証情報に認証情報有効期限と乱数を付加して設定するため、クライアントからサーバへ送信する認証情報の一意性が高くなるという効果を有する。その結果、その認証情報を用いてクライアントのなりすましが不可能となる。

【００２１】また、本発明は、認証情報の一意性を実現するための情報をクライアントのみで設定できるため、クライアントからサーバへ一方向に送信する認証情報で、認証情報の一意性が実現できるという効果を有する。このため、認証のためのクライアントとサーバ間通信が簡単になる。

【図面の簡単な説明】

【図１】本発明のネットワーク利用者認証方式の実施の形態を示すブロック図である。

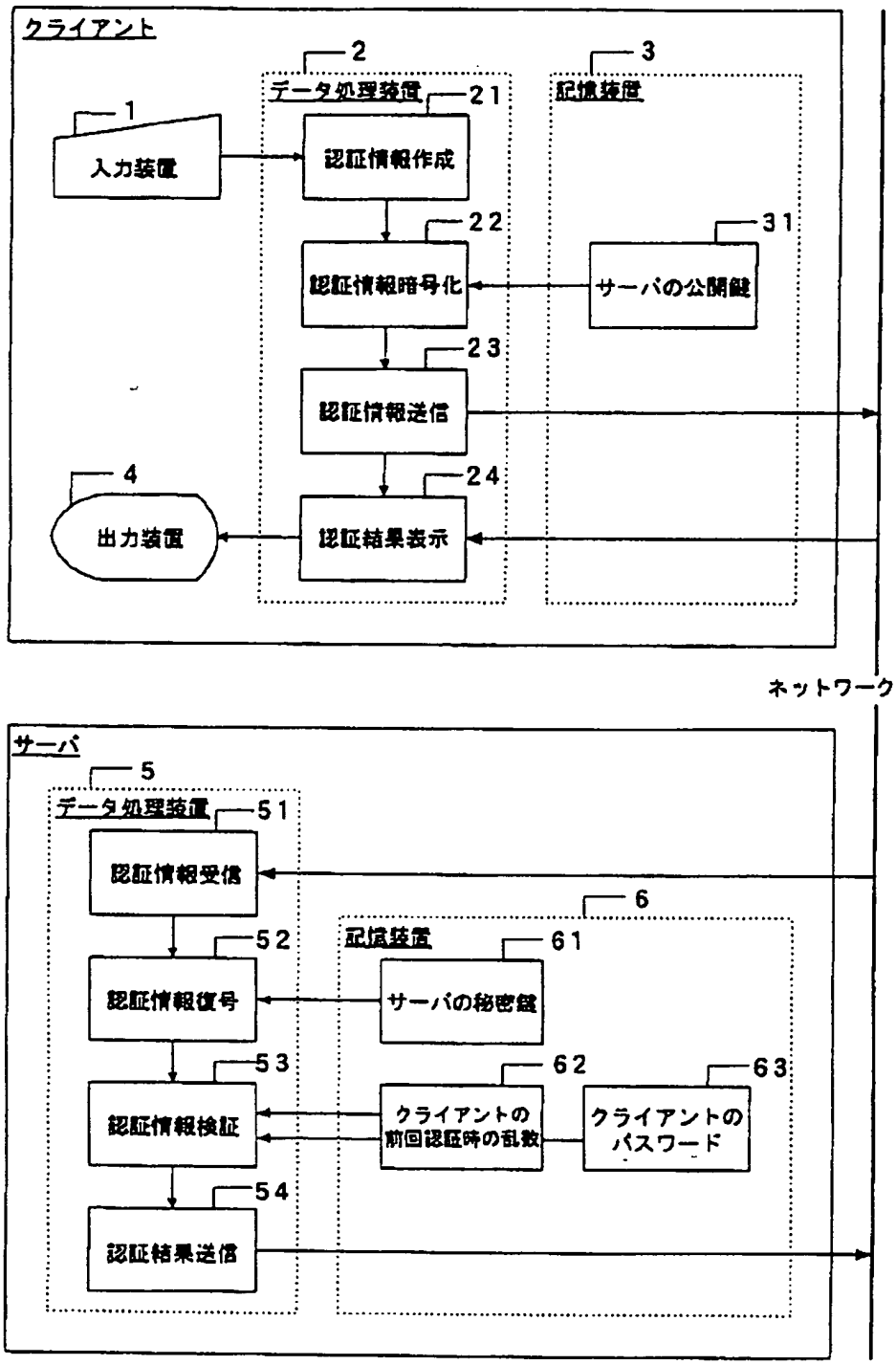
【図２】本発明の実施の形態の動作を説明するフローチャートである。

【図３】本発明の一実施例を示すブロック図である。

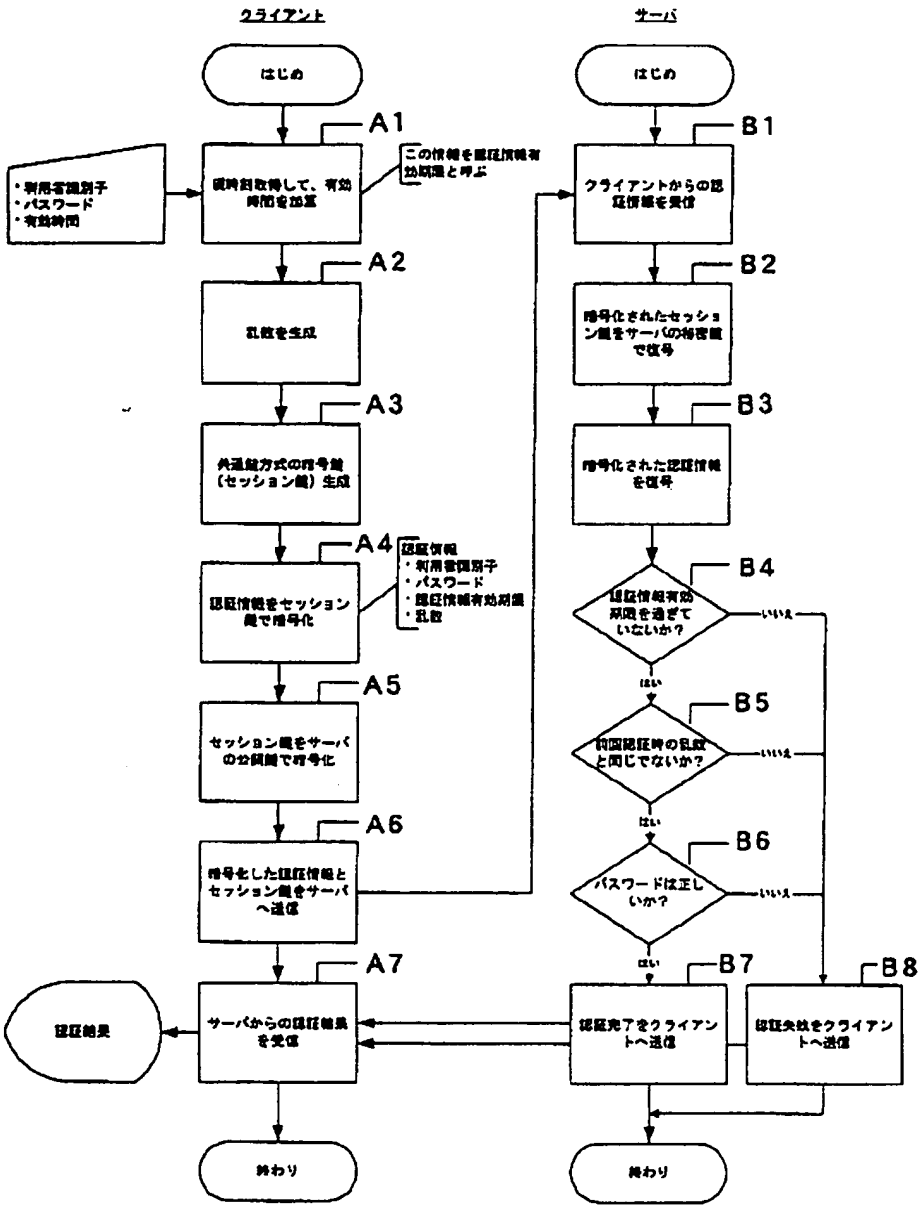
【符号の説明】

１　入力装置
２　データ処理装置
３　記憶装置
４　出力装置
５　データ処理装置
６　記憶装置
２１　認証情報作成
２２　認証情報暗号化
２３　認証情報送信
２４　認証結果表示
３１　サーバの公開鍵
５１　認証情報受信
５２　認証情報復号
５３　認証情報検証
５４　認証結果送信
６１　サーバの秘密鍵
６２　クライアントの前回認証時の乱数
６３　クライアントのパスワード

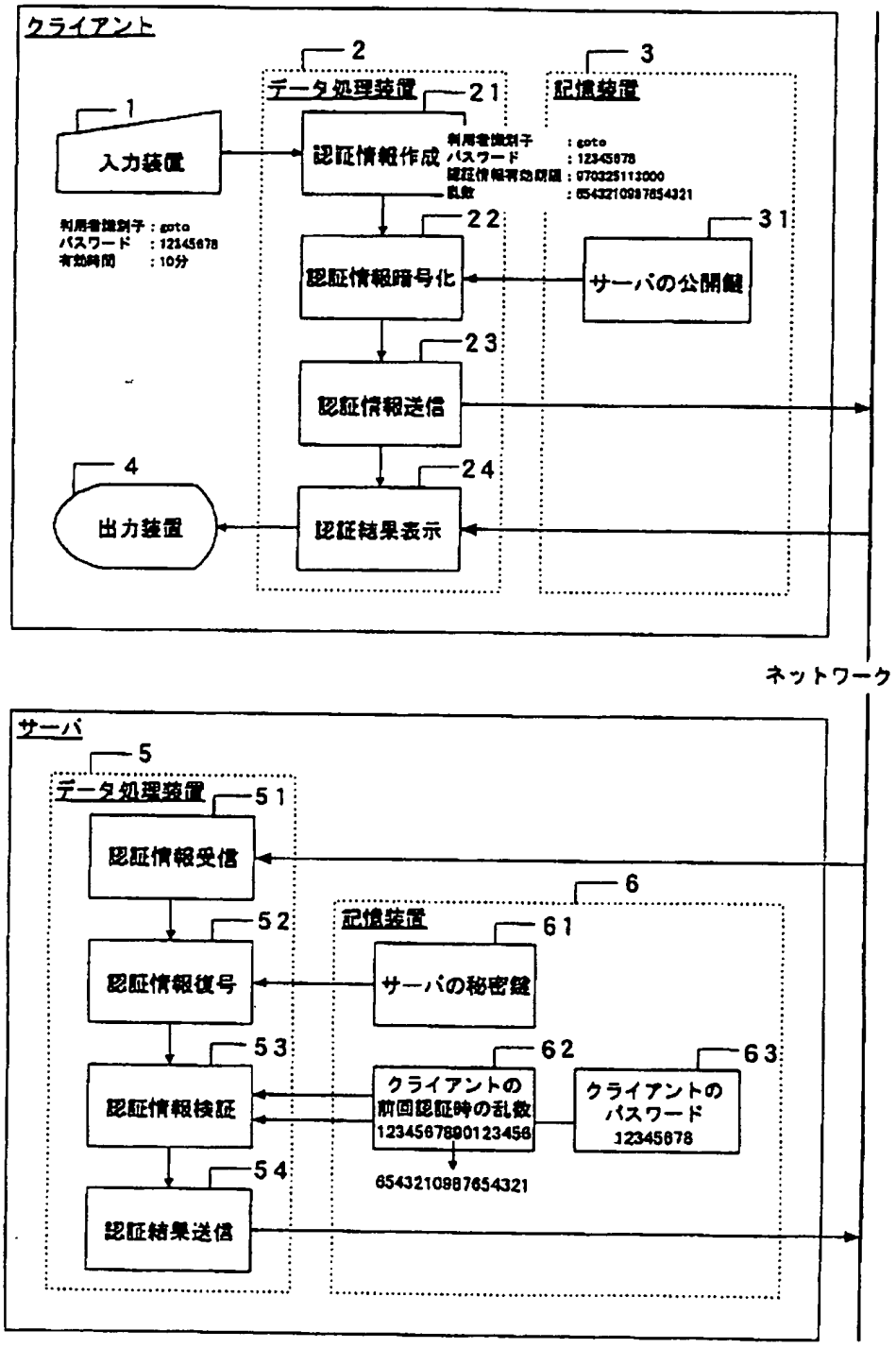
【図1】


クライアント
2
データ処理装置
21
認証情報作成
1
入力装置
3
記憶装置
22
認証情報暗号化
31
サーバの公開鍵
23
認証情報送信
4
出力装置
24
認証結果表示
ネットワーク
サーバ
5
データ処理装置
51
認証情報受信
6
記憶装置
52
認証情報復号
61
サーバの秘密鍵
53
認証情報検証
62
63
クライアントの前回認証時の乱数
クライアントのパスワード
54
認証結果送信

【図２】


クライアント
サーバ
はじめ
はじめ
A1
B1
・利用者識別子
・パスワード
・有効時間
現時刻取得して、有効時間を加算
この情報を認証情報有効期限と呼ぶ
クライアントからの認証情報を受信
A2
B2
乱数を生成
暗号化されたセッション鍵をサーバの秘密鍵で復号
A3
B3
共通鍵方式の暗号鍵（セッション鍵）生成
暗号化された認証情報を復号
A4
B4
認証情報
・利用者識別子
・パスワード
・認証情報有効期限
・乱数
認証情報をセッション鍵で暗号化
認証情報有効期限を過ぎていないか？
いいえ
はい
A5
B5
セッション鍵をサーバの公開鍵で暗号化
前回認証時の乱数と同じでないか？
いいえ
はい
A6
B6
暗号化した認証情報とセッション鍵をサーバへ送信
パスワードは正しいか？
いいえ
はい
A7
B7
B8
認証結果
サーバからの認証結果を受信
認証完了をクライアントへ送信
認証失敗をクライアントへ送信
終わり
終わり

【図３】


クライアント
2
データ処理装置
21
3
記憶装置
1
入力装置
認証情報作成
利用者識別子　：goto
パスワード　：12345678
認証情報有効期限：970325113000
乱数　：6543210987654321
利用者識別子：goto
パスワード　：12345678
有効時間　：10分
22
31
認証情報暗号化
サーバの公開鍵
23
認証情報送信
4
24
出力装置
認証結果表示
ネットワーク
サーバ
5
データ処理装置
51
認証情報受信
6
記憶装置
61
52
認証情報復号
サーバの秘密鍵
53
62
63
認証情報検証
クライアントの
前回認証時の乱数
1234567890123456
クライアントの
パスワード
12345678
6543210987654321
54
認証結果送信